Remarks by

Thomas J. Curry
Comptroller of the Currency

Before the
Institute of International Bankers
Annual Washington Conference

Washington, DC
March 4, 2013

Thank you. It's a pleasure to be here with you today. The IIB's Washington conferences always provide a good forum to discuss important policy issues, and I'm glad to have this time to talk to you about what I consider to be one of the most significant regulatory matters before us today.

That issue is operational risk, which we define as the risk of losses from the failure of people, processes, systems, and external events. Operational risk is embedded in virtually every activity a financial institution engages in, from check processing to trading activities, and the more complex the institution or process, the greater the risk of operational failure. Today, markets and information technology systems are growing increasingly complex, and so it should probably come as no surprise that the OCC views operational risk as a high and growing concern.

But it's truly extraordinary that operational risk is at the top of our safety and soundness concerns for the large banks we supervise. Some of our most seasoned supervisors, people with 30 or more years on the job, tell me that this is the first time they've seen operational risk eclipse credit risk as a safety and soundness concern. I agree. For almost the entire time I've been involved in bank supervision, it's been a truism that banks succeed or fail based on how well they manage credit risk. Today,

though, we are seeing banks and thrifts of all sizes, and large ones in particular, struggle with risks that arise from the failure of people and processes.

I'm sure you know the areas I have in mind: debt collection practices, trading operations, Bank Secrecy Act compliance, and mortgage servicing, among others. Each of these issues has absorbed management time and resources that could be better spent on other matters, and they have resulted in enforcement actions and damage to the institution's reputation.

I'd like to focus the remainder of my remarks on one particular area involving operational risk, namely the risk that arises from the failure to maintain effective Bank Secrecy Act and Anti-Money Laundering compliance programs.

There's nothing new about BSA/AML compliance. The Bank Secrecy Act was passed into law in 1970, and it's been augmented over the years by additional legislation, including the Money Laundering Control Act of 1986, which provides a framework for BSA/AML supervision and enforcement, and the USA PATRIOT Act.

Despite its long history, BSA/AML compliance sometimes seems like a lesson that all of us learn over and over again. I had barely begun my career in state government in Massachusetts when one of the most prominent banks in our state, First National Bank of Boston, pleaded guilty to failing to report $1.2 billion in currency transactions with Swiss banks and paid what was then the largest fine ever imposed for BSA violations – $500,000. That was in 1985, and the case was the subject of months of headlines and congressional investigations. It came as a shock to many who were learning about the Bank Secrecy Act for the first time.

Since then, we've had a number of high visibility cases, from Riggs Bank in 2004 to Wachovia Bank in 2010. Those institutions were hardly alone. From 2005 to 2010, the OCC issued 41 cease and desist orders against national banks under our supervision for failure to maintain adequate BSA programs.

However, in the past two years, we've found surprising deficiencies at some of our very largest institutions. HSBC, JPMorgan Chase, and Citibank have all been subject to enforcement actions. And the civil money penalties we have imposed make Bank of Boston's $500,000 fine look tiny. Indeed, the CMP assessed against HSBC was a thousand times larger – $500 million – and represents the largest money penalty ever assessed by a federal banking agency. More importantly, it exceeded by a very wide margin any of the savings the bank may have realized by cutting corners.

Some have questioned whether the resurgence of problems in this area is because the financial crisis distracted all of us – financial institutions and regulators alike – from compliance concerns. I would say that while that might explain some of the deficiencies, it can't be allowed to excuse them.

The Bank Secrecy Act was passed to provide another tool in the battle against illicit drugs, but today it has become a major weapon in the war on terrorism. The information that we gain from reports filed as a result of effective BSA/AML and OFAC programs provides an invaluable tool for finding and tracking terrorist activities.

Many of the largest institutions have implemented highly sophisticated programs and systems that screen transactions to identify and report suspicious activity to law enforcement, and to ensure that such transactions do not involve entities subject to OFAC sanctions. More than 5.6 million SARs have been collected in the centralized database

that is maintained by the Financial Crimes Enforcement Network, or FinCEN, and these reports provide critical information to law enforcement agencies. The majority of these SARs have been filed by national banks and federal thrifts.

But there is still a question as to why so many sophisticated banks – many of which spend hundreds of millions of dollars on BSA compliance – have fallen short. In fairness, BSA compliance is inherently difficult. It involves the challenge of sifting through large volumes of transactions to identify those with suspicious features, a task made especially difficult by the ingenuity criminal elements have shown concealing the true nature of the transactions they undertake.

As banks' BSA compliance programs have evolved and changed over time, so has the sophistication and determination of criminal elements that are looking for access to our financial system. The technology, products, and services that you and other banks offer to give your customers better and quicker access to financial services can also be used by criminals to instantaneously and anonymously move money throughout the world, sometimes through the simple click of a keypad or the use of a cell phone app.

Risks are constantly mutating, as criminal elements alter their tactics to avoid detection. The bad guys have ample resources, and they move quickly from one base of operations to another, finding sanctuary in places where law enforcement, or sympathy for U.S. policy objectives, is weakest. Illicit funds are like flowing water in that they go to the point of least resistance and continually move and change direction from one institution to the next. To assist and encourage this flow, money laundering schemes have had to become more sophisticated and complex, involving entities and individuals located in numerous jurisdictions worldwide. Consequently, banks, thrifts, and other

financial institutions have had to devote increasingly larger amounts of resources to maintain effective programs to prevent this flow.

So clearly, it's going to be a challenge, for financial institutions, regulators, and law enforcement, to stay ahead of the curve. Right now, we're seeing a number of trends and areas of concern that warrant close attention by both regulators and banks.

First is the lack of compliance resources. In many of the most recent cases, our examiners concluded that the institution failed to commit adequate resources to its BSA/AML program. Austerity programs have led to a reduction of staff and other resources at some banks, and at others, programs have failed to keep pace with the institution's growth.

A second area involves international activities. Foreign correspondent banking, cross border funds transfers, bulk cash repatriation, remote deposit capture, and embassy banking have all been high-risk areas that some banks have not managed effectively. Going back a few years, the failure of Riggs to manage its embassy banking program ultimately led to the demise of one of the nation's most storied banks. Controls in this area need to be commensurate with the risks.

Third-party relationships and payment processors also require attention. BSA isn't the only area in which banks have stumbled because they failed to monitor work that was being done on their behalf by third parties, but it's one with perhaps the most significant consequences. The OCC and the other banking agencies have been monitoring this area closely over the years, and we have issued risk management guidance to prevent problems, and we've taken enforcement actions when we've found problems.

In addition, there's a significant risk that these activities will migrate to smaller banks and thrifts as larger institutions improve their programs and exit businesses that present elevated levels of risk. Smaller institutions may lack the resources and personnel necessary to successfully manage higher-risk activities, and so they need to be especially vigilant.

The last trend I want to highlight involves new technologies and evolving payment activities. As banks and thrifts introduce new technology, it's vital that they understand the compliance risk.

The Internet is the most obvious example, but it's not the only one. Think about the development of new payment systems, some of which exist outside the banking and thrift industries. PayPal has become a familiar payment mechanism for many of us, especially when we make a purchase on the Internet, and you see more and more people every day paying for coffee at Starbucks by flashing their Smartphone at a scanner. In fact, a bank account today can consist of nothing more than a plastic card that is capable of receiving paychecks, paying bills, and storing money.

All of these innovations add to consumer convenience, and financial institutions that want to remain competitive will find it necessary to offer products that take advantage of new technology. But some of them also bring compliance risk. For example, how do we track illicit money when it can be loaded onto cards and moved over the Internet?

Prepaid access cards, mobile phone banking, smart ATM machines and kiosks, mobile wallets, and Internet cloud-based payment processes are all technologies that are developing rapidly. Senior bank compliance personnel need to be involved in the product

development process to ensure that their institution is appropriately managing the risk these technologies entail. Monitoring for compliance with requirements of the OFAC is especially important – and particularly challenging – in this area.

The bad guys have both the resources and the incentives to try to stay a step ahead, so we and banks have to continually improve our programs. Our experience indicates there are four critical ingredients for a sound BSA/AML program: the strength of an institution's compliance culture, its willingness to commit sufficient resources, the strength of its information technology and monitoring processes, and its risk management.

The health of a bank's culture starts at the top, and so it's important that senior management demonstrate a commitment to BSA/AML compliance. Employees need to know BSA compliance is a management priority and that it will receive the resources it needs to succeed, including training and first rate information technology.

In that regard, I'd like to commend the Institute for the seminars and conferences you sponsor on BSA/AML issues. I know that members of our staff at the OCC have participated in these conferences over the years, and these events not only highlight the importance of effective compliance programs, but they help keep your members up to date on current developments.

And both of those objectives are vitally important. For our part, we will continue to improve our supervision, but we recognize there is much work to be done. In this regard, we will continue to work with the other agencies to ensure that our examination policies remain up to date and our risk management guidance remains current. In 2005, we published an interagency BSA/AML manual that effectively standardized

examination procedures for the federal banking agencies, and we have revised the manual three times since then to make sure it reflects the latest technological and payment system innovations, as well as emerging threats and vulnerabilities. We will continue to work with our colleagues at the other agencies to ensure that the manual remains current in its procedures and focused on the right issues.

The fact is, terrorists and criminal elements will continue to devote money and effort to finding ways into the banking and payment systems, and so we must continue to improve our efforts to keep them out. That will require resourcefulness as well as resources, and most of all, vigilance and the sheer determination to win. It's not an easy task, but it's one that all of us are up to. I'm confident that we will succeed.

Thank you. I'd be happy to take a few questions.